(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
13 octobre 2005 (13.10.2005)

(10) Numéro de publication internationale
WO 2005/096135 A3

(51) Classification internationale des brevets[7] : G06F 7/52

(21) Numéro de la demande internationale :
PCT/FR2005/000443

(22) Date de dépôt international :
24 février 2005 (24.02.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0402146 2 mars 2004 (02.03.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **LEFRANC, David** [FR/FR]; Résidence Stéphanolyse, 7, rue des Tilleuls, F-14000 Caen (FR).

(74) Mandataires : **LOISEL, Bertrand** etc.; Cabinet Plasseraud, 65/67, rue de la Victoire, F-75440 Paris Cedex 09 (FR).

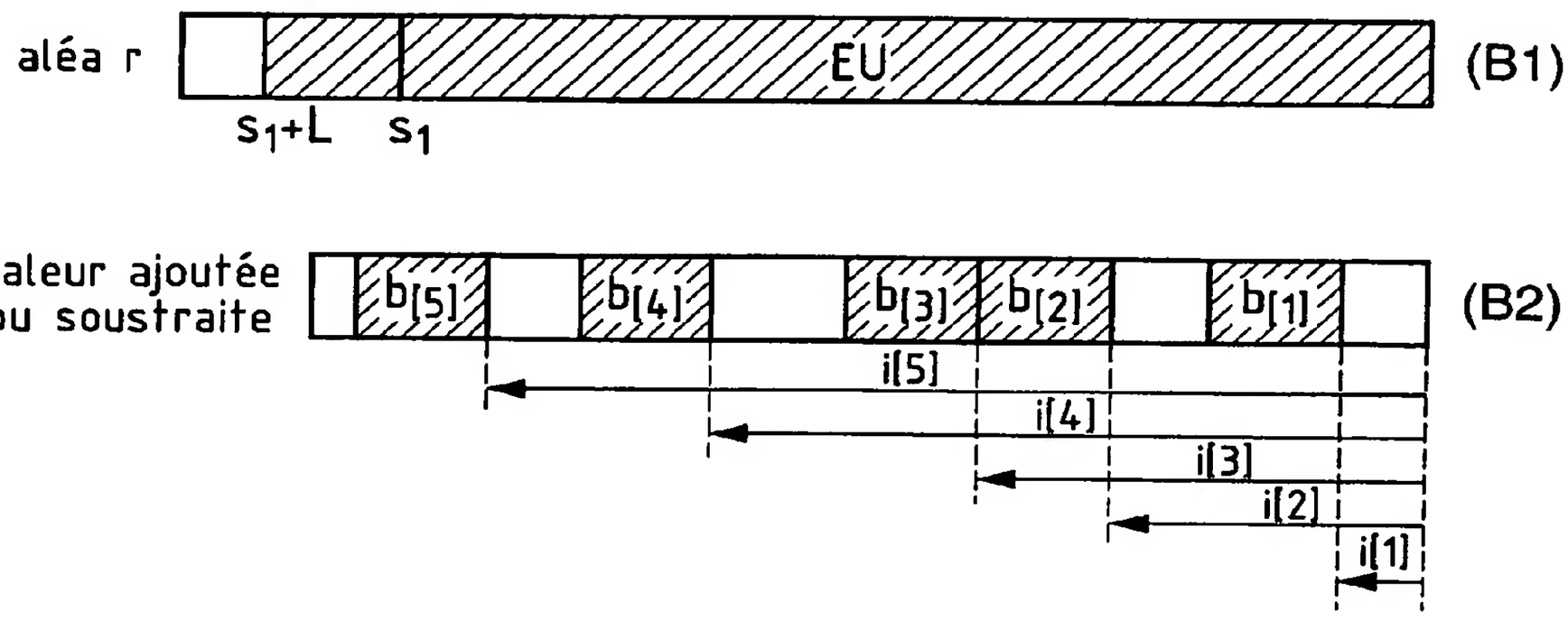
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,

[Suite sur la page suivante]

(54) **Title:** METHOD AND DEVICE FOR PERFORMING A CRYPTOGRAPHIC OPERATION

(54) **Titre :** PROCEDE ET DISPOSITIF POUR ACCOMPLIR UNE OPERATION CRYPTOGRAPHIQUE



(B1) ... RANDOM
(B2) ... INCREMENT OR SUBTRACTED VALUE

(57) **Abstract:** The inventive method for performing a cryptographic operation by a device controlled by the security application executed outside thereof consists in producing a cryptographic value (y) in the device by a calculation comprising at least one multiplication between first and second factors containing a security key (s) associated with the device and a challenge number (c) provided by the security application. The first multiplication factor comprises a determined number of bits (L) in a binary representation. The second factor is constrained in such a way that it comprises; in a binary representation, several bits at 1 with a sequence of at least L-1 bits at 0 between each pair of consecutive bits to 1 and the multiplication is carried out by assembling the binary versions of the first factor shifted according to positions of the bits at 1 of the second factor, respectively.

[Suite sur la page suivante]

WO 2005/096135 A3

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) Date de publication du rapport de recherche internationale: 6 avril 2006

(15) Renseignements relatifs à la correction:
Correction précédente:
voir la Gazette du PCT n° 49/2005 du 8 décembre 2005

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Pour accomplir une opération cryptographique dans un dispositif sous le contrôle d'une application de sécurité exécutée en dehors du dispositif, on produit une valeur cryptographique (y) dans le dispositif, par un calcul comprenant au moins une multiplication entre des premier et second facteurs incluant une clé secrète (s) associée au dispositif et un nombre (C) dit challenge fourni par l'application de sécurité. Le premier facteur de la multiplication comprend un nombre de bits déterminé L en représentation binaire. On contraint le second facteur pour qu'il comprenne, en représentation binaire, plusieurs bits à (1) avec, entre chaque paire de bits à (1) consécutifs, une séquence d'au moins L-1 bits à (0), et en ce que la multiplication est réalisée en assemblant des versions binaires du premier facteur respectivement décalées conformément aux positions des bits à (1) du second facteur.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR2005/000443

A. CLASSIFICATION OF SUBJECT MATTER
G06F7/52

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 995 082 A (SCHNORR ET AL) 19 February 1991 (1991-02-19) page 2, line 31 - page 4, line 10 page 9, line 25 - line 35 -----	1-23
A	US 2003/093671 A1 (OWLETT JOHN) 15 May 2003 (2003-05-15) paragraph [0026] - paragraph [0034] -----	1-23
A	US 2003/159038 A1 (GILBERT HENRI ET AL) 21 August 2003 (2003-08-21) paragraph [0005] - paragraph [0015] -----	1-23

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 January 2006	30. 01. 2006

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Prins, L

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR2005/000443

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4995082 A	19-02-1991	AT 106643 T	15-06-1994
		DE 59005851 D1	07-07-1994
		EP 0383985 A1	29-08-1990
		EP 0384475 A1	29-08-1990
		ES 2054120 T3	01-08-1994
		JP 2666191 B2	22-10-1997
		JP 3001629 A	08-01-1991
US 2003093671 A1	15-05-2003	NONE	
US 2003159038 A1	21-08-2003	AT 268034 T	15-06-2004
		DE 60103515 D1	01-07-2004
		DE 60103515 T2	30-06-2005
		EP 1266364 A1	18-12-2002
		ES 2221642 T3	01-01-2005
		FR 2806858 A1	28-09-2001
		WO 0171675 A1	27-09-2001
		JP 2003528515 T	24-09-2003

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR2005/000443

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

G06F7/52

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

G06F H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 4 995 082 A (SCHNORR ET AL) 19 février 1991 (1991-02-19) page 2, ligne 31 - page 4, ligne 10 page 9, ligne 25 - ligne 35 -----	1-23
A	US 2003/093671 A1 (OWLETT JOHN) 15 mai 2003 (2003-05-15) alinéa [0026] - alinéa [0034] -----	1-23
A	US 2003/159038 A1 (GILBERT HENRI ET AL) 21 août 2003 (2003-08-21) alinéa [0005] - alinéa [0015] -----	1-23

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
23 janvier 2006	30. 01. 2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Prins, L

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR2005/000443

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 4995082 A	19-02-1991	AT 106643 T	15-06-1994
		DE 59005851 D1	07-07-1994
		EP 0383985 A1	29-08-1990
		EP 0384475 A1	29-08-1990
		ES 2054120 T3	01-08-1994
		JP 2666191 B2	22-10-1997
		JP 3001629 A	08-01-1991
US 2003093671 A1	15-05-2003	AUCUN	
US 2003159038 A1	21-08-2003	AT 268034 T	15-06-2004
		DE 60103515 D1	01-07-2004
		DE 60103515 T2	30-06-2005
		EP 1266364 A1	18-12-2002
		ES 2221642 T3	01-01-2005
		FR 2806858 A1	28-09-2001
		WO 0171675 A1	27-09-2001
		JP 2003528515 T	24-09-2003